(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/05224 A2

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number: PCT/US01/21725

(22) International Filing Date: 10 July 2001 (10.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/217,243 10 July 2000 (10.07.2000) US
60/217,202 10 July 2000 (10.07.2000) US

(71) Applicant: PAYPAL, INC. [US/US]; 1840 Embarcadero Road East, Palo Alto, CA 94303 (US).

(72) Inventors: TEMPLETON, James; 2909 Postwood Drive, San Jose, CA 95132 (US). BHARGAVA, Sanjay; 188 Fleetwood Drive, San Carlos, CA 94070 (US).

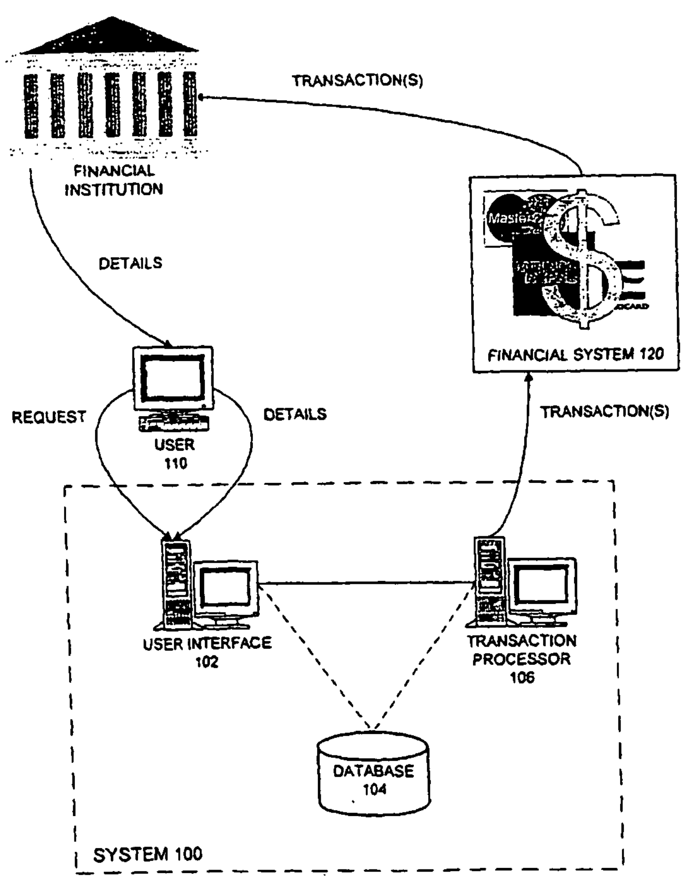
(74) Agents: VAUGHAN, Daniel et al.; Park, Vaughan & Fleming LLP, 702 Marshall Street, Suite 310, Redwood City, CA 94063 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR VERIFYING A FINANCIAL INSTRUMENT



(57) Abstract: A system and method for verifying a financial instrument or a user's authorization to use a financial instrument. A transaction processor initiates one or more verifying transactions involving the instrument, with details that may vary from one transaction to another, such as the type of transaction (e.g., deposit, credit, debit), amount of the transaction, number of transactions, the merchant or vendor name or account for the transaction, and so on. Selected details, particularly variable ones, are saved in the system. Th user accesses information regarding the transaction by accessing it on-line, via telephone, in a monthly statement, etc. The user then submits the requested details to the system through a user interface, which compares them to the stored details. If they correspond, then the user may be permitted to use the instrument (e.g., for a purchase, a fund transfer).

WO 02/05224 A2

SYSTEM AND METHOD FOR VERIFYING A FINANCIAL INSTRUMENT

BACKGROUND

This invention relates to the fields of computer systems and data communications. More particularly, a system and method are provided for verifying financial instruments or accounts, such as credit cards, debit cards, bank accounts, etc.

Modern financial systems make it easy to perform financial transactions without using physical currency. For example, credit cards and ACH (Automated Clearing House) transactions (i.e., electronic checks) are increasingly used in place of cash to make purchases, transfer money, or engage in other financial transactions.

These convenient instruments are, however, subject to theft and fraudulent use. A thief may obtain all the information needed to use a stolen credit card from the card itself, while all that is needed to conduct an ACH transaction (e.g., to withdraw money from a checking account) are the bank account and routing numbers from a check. It is then a simple matter for the thief or fraud artist to pose as the rightful owner or holder of a credit card or bank account. Existing safeguards against fraud (e.g., checking a credit card against a list of stolen cards, checking the name on a checking account before completing an ACH transaction) are often insufficient. It is typically the merchant, vendor, bank or other entity that accepts a credit card or electronic check transaction that is liable for the amount of money that is stolen or misappropriated if the rightful owner or holder is not at fault.

SUMMARY

Therefore, in one embodiment of the invention a system and method are provided for verifying financial instruments or accounts, such as credit or debit cards, bank accounts, and so on, in order to ensure that a person attempting to use such an instrument is authorized to do so.

When a customer or user expresses a desire to use a certain instrument (e.g., to make purchases or fund transfers), the system initiates one or more verifying transactions using the instrument. Selected details of the transaction(s) are saved, particularly details

hardware utilizing either a combination of microprocessors or other specially designed application specific integrated circuits, programmable logic devices, or various combinations thereof. In particular, the methods described herein may be implemented by a series of computer-executable instructions residing on a suitable computer-readable medium. Suitable computer-readable media may include volatile (e.g., RAM) and/or non-volatile (e.g., ROM, disk) memory, carrier waves and transmission media (e.g., copper wire, coaxial cable, fiber optic media). Exemplary carrier waves may take the form of electrical, electromagnetic or optical signals conveying digital data streams along a local network or a publicly accessible network such as the Internet.

In one embodiment of the invention, a system and method are provided for verifying a financial instrument or account or verifying a user's authorization to use a financial instrument or account. A financial instrument or account may be defined to include credit cards, debit cards, bank accounts, brokerage accounts, money market accounts, and so on – virtually any entity that may be used as a source or destination of electronically exchanged value.

More particularly, a system and method of the invention may be applied to ensure that a financial instrument identified by a user (e.g., as a source of funds) is actually owned or controlled by the user. The likelihood or risk that the user has stolen the instrument, and is now attempting to use it fraudulently, may therefore be determined to be lower than if the verification was not performed.

In an embodiment of the invention, a series of transactions are performed using the instrument identified by the user. The transactions may include debits or credits to a credit card, deposits or withdrawals from a bank account, etc. Certain details of the transactions are recorded (e.g., amount, type of transaction, merchant identity, date or time of a transaction) and the user is invited to retrieve specified details (e.g., from an account statement, by calling the holder or issuer of the instrument) and identify them to the system. If the user correctly identifies the specified details, the verification process is successful. If the user is unsuccessful, he or she may be given a limited number of additional opportunities to input the correct details and, if still unsuccessful, may be barred from using the instrument. In this embodiment, the user is required to pass his or her financial institution's own verification/authentication process in order to obtain the necessary details of the transactions, thereby making it even less likely that he or she is a fraudulent user.

account for immediate or future use as a source or destination of funds. User interface 102 may be configured to accept connections via publicly available networks (e.g., the Internet), private networks and other dedicated or shared links, which may be wired or wireless.

Transaction processor 106 is coupled to one or more financial systems or entities for processing financial transactions. Thus, financial system 120 may comprise an ACH (Automated Clearing House) vendor (e.g., a Treasury Management Service configured to handle ACH transactions such as electronic checks and deposits), a merchant acquirer or Treasury Management Service that handles credit card and/or debit card transactions, or some other entity. As specified above, system 100 may include multiple transaction processors. Each transaction processor may be configured for a different type of financial instrument and may interact with a different financial system or entity. Transaction processor 106 may be a separate or specialized element of system 100 (e.g., a computer server) or may be incorporated into another element of the system (e.g., a data server, web server).

Financial system 120 is coupled to the user's financial institution corresponding to the financial instrument being verified. Financial institution 130 may therefore be the user's bank, credit card issuer, brokerage, investment manager, etc. Financial system 120 may, in an embodiment of the invention, represent a collection of financial institutions and entities that communicate with each other by specified formats (e.g., for credit card, debit card and/or ACH transactions). Thus, financial system 120 may comprise financial institution 130.

In one method of verifying a user's financial instrument or account through system 100, user 110 connects to system 100 and identifies an instrument or account that he or she would like to use (e.g., as a source of funds for purchases or money transfers). User interface 102, or the server operating the user interface, passes the identifying information to transaction processor 106. Transaction processor 106 initiates one or more transactions, using variable details such as an amount of the transaction, type of transaction (e.g., deposit, withdrawal, debit, credit), different vendor names or identities, or other details that may be reported to or retrieved by a valid user or owner of the instrument. The transaction may be generated or constructed by user interface 102, transaction processor 106 or some other entity within system 100 (e.g., an application or

partner may allow the entity to specify a merchant name, account, or other detail to be part of the transaction.

Advantageously, the use of variable or different merchant names facilitates the use of an embodiment of the invention internationally. In particular, even if the verifying transactions are initiated in one currency and, at the user's end are converted into another currency, the merchant name or other variable identity can still be used as a verifying detail.

If the manner in which verification transactions are handled causes some of the transaction information to be truncated or excised, the verification system (e.g., system 100 of FIG. 1) may structure transactions accordingly or take that handling into account when comparing stored transaction details against the details offered by a user. For example, if it is likely that part of a vendor name or account will be truncated, then that portion of a transaction may be reported in a way that prevents truncation of disambiguating information (e.g., by using a vendor name of "2468AcmeCorporation" instead of "AcmeCorporation2468"). Then, as long as the user can provide the "2468Acme" portion, this may be considered to match the account name.

FIG. 2 demonstrates one method of verifying a user's specified financial instrument or verifying the user's authority to use the instrument, according to one embodiment of the invention. In this embodiment, a user selects a credit card, debit card, bank account or other account that offers electronic checking or deposits, to be the source of funds for purchases, money transfers or other transactions at a merchant (or other entity).

In order to use variable or different merchant or vendor names/accounts for verifying transactions (as described above), the merchant may, prior to the illustrated method, establish multiple accounts with its credit card issuer or ACH vendor.

In state 202 of the method of FIG. 2, a user (or a user's agent) connects to the verification system, which may be implemented as part of an on-line or traditional merchant or, another entity that accepts payment in forms other than physical currency. This connection may be the user's initial contact with the system, in which case he or she may (or may be required to) verify a source of funds as part of a registration process. Or, this may be just one of many visits, but the user may be requesting a transaction (e.g., a purchase or fund transfer) that requires verification.

In one embodiment of the invention, a typical series of verifying transactions may include two deposits (to a bank account) or credits (to a credit card), each of which is between $ 0.01 and $ 0.99 in value, and may involve different merchant identities (e.g., 1234XYZCorporation, 5160XYZCorporation). To decrease the cost of performing transactions in this embodiment, one or both of the deposit/credit amounts may be biased toward the lower end of the value range.

In state 210, selected details (e.g., all or a subset of the variable details) of the transactions are saved (e.g., stored in a database) and the transactions are initiated (e.g., through transaction processors coupled to the appropriate financial systems or entities). The verifying transactions may be initiated all at the same time, may be separated in time or sent through different financial systems or entities. Also, the verifying transactions may be joined with other transactions (e.g., a verifying deposit may be merged with a subscription fee being charged to the user), in which case details of the merged transactions would be saved for comparison with the details reported by the user.

In optional state 212, the user may be notified (e.g., via electronic mail) that he or she should wait for or retrieve evidence of the transactions. The user may be notified when, or shortly after, the transaction is initiated. Or, the user may be notified after enough time has passed for the transaction to be completed.

The user's evidence of the transaction(s), which should include all or a subset of the details of the transaction(s), may be in the form of a monthly statement mailed to the user from his or her financial institution. Or, the user may take a more proactive approach and access his or her instrument or account status on-line or via telephone. In some manner, the user obtains information regarding the transaction(s).

In state 214 the user (or an agent of the user) connects to the system and, in state 216, proffers or provides supposed details of the verifying transaction(s). Illustratively, the system (e.g., a user interface) may prompt the user to enter the amount of each transaction, the merchant name (or the variable part thereof), the type of transaction, and/or any other detail that was stored.

In this embodiment, the system is configured to communicate with the user through a user interface. However, in alternative embodiments the user may be able to interact with human operators for all or any part of the verification process.

What Is Claimed Is:

1. A method of verifying a customer's authority to use a financial instrument, comprising:

initiating one or more transactions using a financial instrument identified by a customer;

storing one or more attributes of said one or more transactions;

receiving a set of proffered attributes;

comparing said proffered attributes to said stored attributes; and

accepting use of the financial instrument by the customer if said proffered attributes match said stored attributes.

2. The method of claim 1, further comprising after said initiating, soliciting said proffered attributes from the customer.

3. The method of claim 1, wherein said initiating comprises:

initiating a first transaction involving the financial instrument with a first set of attributes; and

initiating a second transaction involving the financial instrument with a second set of attributes different from said first set of attributes.

4. The method of claim 1, wherein said storing attributes comprises storing a value of a first transaction in said one or more transactions.

5. The method of claim 1, wherein said storing attributes comprises storing a merchant identity of a first transaction in said one or more transactions.

6. The method of claim 1, wherein said storing attributes comprises storing the number of said one or more transactions.

7. The method of claim 1, wherein said storing attributes comprises storing a type of one of said one or more transactions.

18. The method of claim 13, wherein the financial account is a savings account.

19. The method of claim 13, wherein the financial account is a bank account.

20. The method of claim 13, wherein said first set of details includes a merchant identity of a first transaction.

21. The method of claim 13, wherein said first set of details includes an amount of a first transaction.

22. The method of claim 13, wherein said first set of details includes a type of a first transaction.

23. The method of claim 13, wherein said first set of details includes the number of said transactions.

24. The method of claim 13, wherein said first set of details includes an identity of an account involved in said transactions, other than the financial account.

25. A method of verifying a credit card, comprising:

receiving from a user an account number and a name identifying a credit card the user wishes to use as a source of funds;

initiating one or more transactions involving the credit card;

storing a first set of details of said transactions;

prompting the user to identify details of said transactions;

receiving from the user a second set of details; and

if said second set of details matches said first set of details, authorizing the user to use the credit card as a source of funds.

26. The method of claim 25, wherein said second set of details includes an identifier of a merchant involved in one of said one or more transactions.

31. The system of claim 30, wherein said processor is further configured to authorize the user to use the external financial account if said test set of details matches a predetermined subset of said first set of details.

32. The system of claim 30, wherein said transaction processor is coupled to an ACH (Automated Clearing House) transaction handler.

33. The system of claim 30, wherein said transaction processor is coupled to a credit card service provider.

34. The system of claim 33, wherein said credit card service provider is a merchant acquirer.

35. The system of claim 33, wherein said credit card service provider is a credit card gateway provider.

36. The system of claim 30, wherein said transaction processor is configured to construct said one or more transactions prior to their initiation.

37. The system of claim 30, further comprising a computer server for operating said user interface.

38. The system of claim 37, wherein said computer server is further configured to construct said one or more transactions prior to their initiation by said transaction processor.

39. An apparatus for verifying a customer's authority to use a financial instrument, comprising:

means for receiving from a customer information identifying a financial instrument;

transaction means for initiating one or more transactions involving the financial instrument;

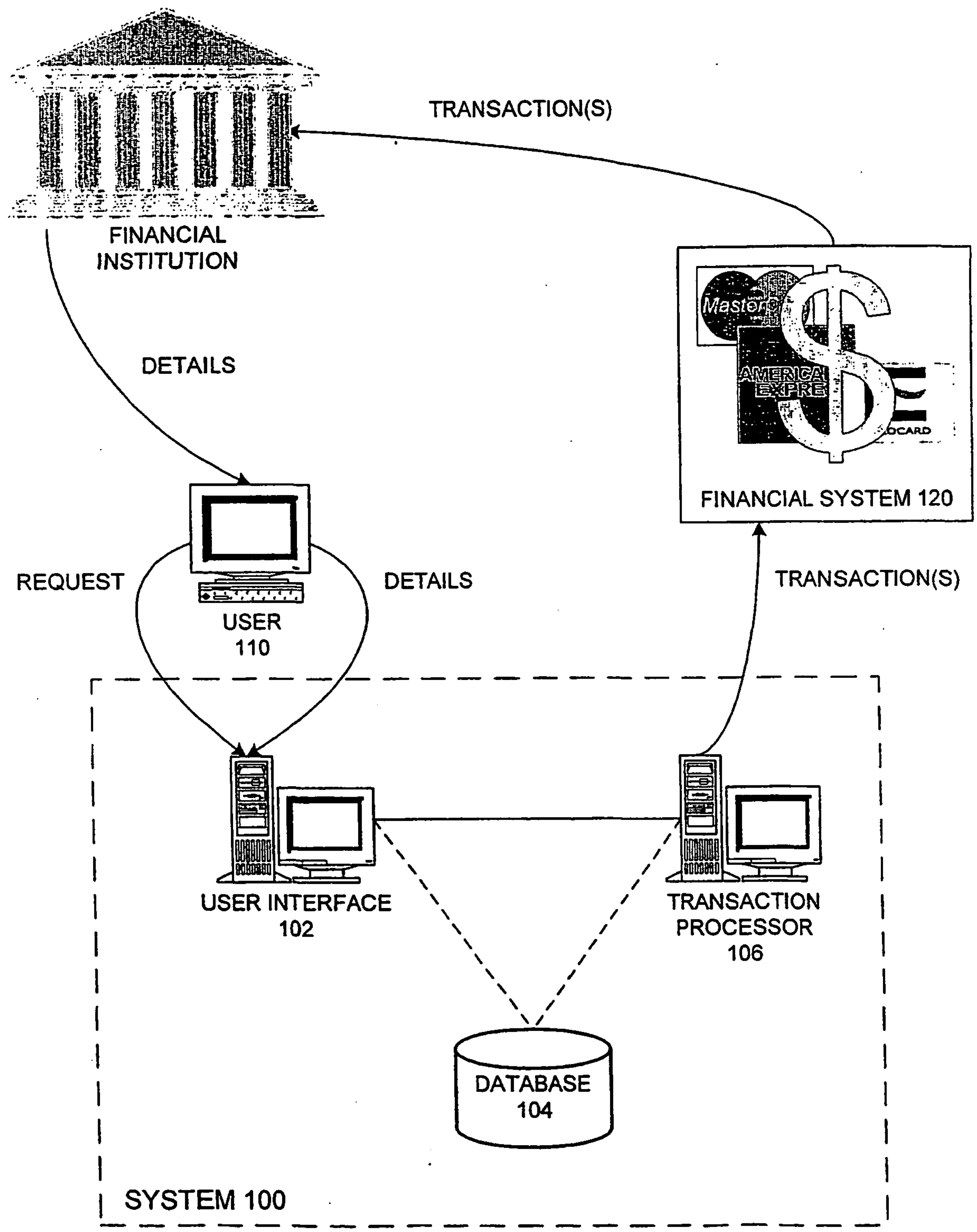

TRANSACTION(S)
FINANCIAL INSTITUTION
DETAILS
FINANCIAL SYSTEM 120
REQUEST
DETAILS
USER 110
TRANSACTION(S)
USER INTERFACE 102
TRANSACTION PROCESSOR 106
DATABASE 104
SYSTEM 100

FIG. 1

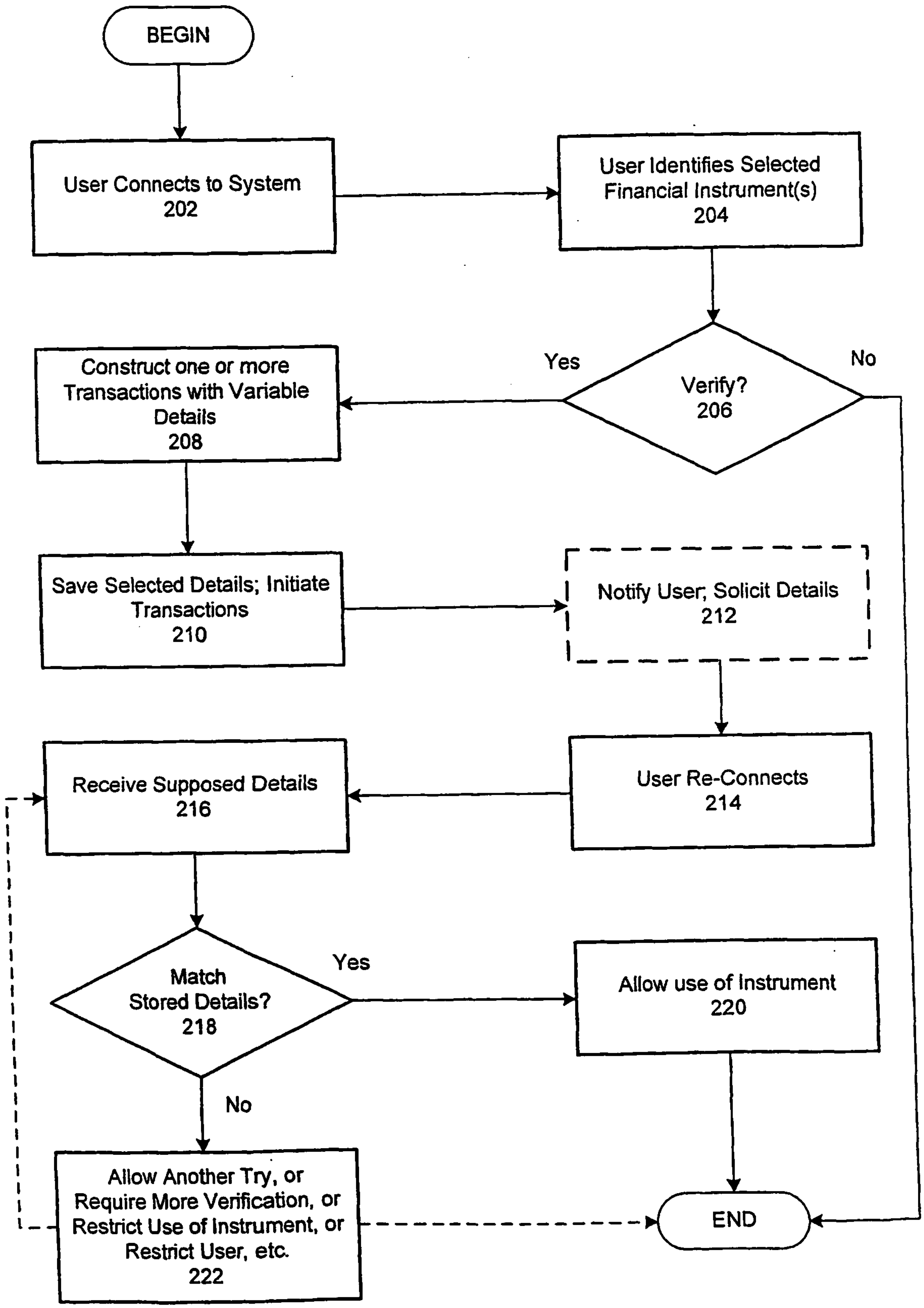

BEGIN
User Connects to System
202
User Identifies Selected
Financial Instrument(s)
204
Yes
Verify?
206
No
Construct one or more
Transactions with Variable
Details
208
Save Selected Details; Initiate
Transactions
210
Notify User, Solicit Details
212
Receive Supposed Details
216
User Re-Connects
214
Match
Stored Details?
218
Yes
Allow use of Instrument
220
No
Allow Another Try, or
Require More Verification, or
Restrict Use of Instrument, or
Restrict User, etc.
222
END

FIG. 2